

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DIVISION OF MISSOURI**

TONI REYNOLDS, <i>on behalf</i>)	Civil Action No.
<i>of herself and all similarly situated persons,</i>)	
)	
Plaintiff,)	
)	CLASS ACTION COMPLAINT
v.)	JURY TRIAL DEMANDED
)	
CORNERSTONE NATIONAL)	
INSURANCE COMPANY,)	
)	
Defendant.)	

CLASS ACTION COMPLAINT

Plaintiff Toni Reynolds (“Plaintiff” or “Plaintiff Reynolds”), individually and on behalf of all others similarly situated, brings this Class Action Complaint (the “Action”) to obtain damages, restitution, and injunctive relief for the Class, as defined below, against Cornerstone National Insurance Company, a Missouri corporation (“Defendant,” or “Cornerstone”). Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This Action arises out of the recent data breach at Cornerstone, an insurance provider, that targeted the information provided by consumers who used or applied for insurance services supplied by Defendant or Defendant’s subsidiaries, subdivisions, or affiliates, or whose information Defendant otherwise had in its possession (the “Data Breach”).

2. The Data Breach resulted in unauthorized access to the data Defendant had in its possession. Because of the Data Breach, approximately 232,391 putative Class members

(including Plaintiff)¹ suffered ascertainable losses including, but not limited to, out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack. In addition, Plaintiff and Class members are now faced with the present and substantial risk of imminent harm caused by the compromise of their sensitive personal information, including their first and last names, driver's license numbers, and other sensitive information from motor vehicle records Defendant obtained in connection with an insurance plan or application for an insurance plan (hereinafter, the "Personally Identifiable Information" or "PII").

3. As a result of the Data Breach Plaintiff and Class members have been harmed and have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now guard against identity theft perpetrated using the stolen first and last names, driver's license numbers, and other sensitive information from motor vehicle records.

4. Plaintiff and Class members may also incur out-of-pocket costs, for example, through having to purchase identity theft protection services, credit freezes, or other protective measures to deter and detect identity theft.

5. Plaintiff seeks to remedy those harms on behalf of herself and all similarly situated persons whose PII was accessed unlawfully during the Data Breach. Plaintiff seeks remedies including, but not limited to, damages (including compensatory and statutory damages), reimbursement for out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate identity theft protection funded by the Defendant.

6. As such, Plaintiff brings this Action against Defendant seeking redress for its unlawful conduct, asserting claims for violations of the Driver's Privacy Protection Act, negligence, negligence *per se*, California's Consumer Protection Act, and California's Unfair Competition Law.

¹ Office of the Maine Attorney General, Data Breach Notifications (Aug. 4, 2022), <https://apps.web.maine.gov/online/aeviewer/ME/40/0e2b3fa0-c37d-4645-afca-54ea90420a0e.shtml> (last visited Sept. 12, 2022).

II. JURISDICTION, VENUE, AND CHOICE OF LAW

A. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act because (1) there are more than 100 putative Class members, (2) the aggregate amount-in-controversy, exclusive of costs and interest, exceeds \$5,000,000.00, and (3) there is minimal diversity because Plaintiff and Defendant Cornerstone are citizens of different states – namely, that Plaintiff is a California resident and the Defendant is a Missouri corporation.

8. Alternatively, this Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 due to Plaintiff's inclusion of claims alleged under the Driver's Privacy Protection Act as well as supplemental jurisdiction over the state law claims alleged pursuant to 28 U.S.C. § 1367, as all claims alleged herein arise from the same case or controversy.

9. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is incorporated in Missouri, and has sufficient minimum contacts with Missouri.

10. In accordance with 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District, Defendant is headquartered in this District, and Defendant transacts business within this District.

11. Application of Missouri law to this dispute is proper because Defendant's headquarters are in Missouri, the decisions or actions that gave rise to the underlying facts at issue in this Complaint were presumably made or taken in Missouri, and the action/or inaction at issue emanated from Missouri.

B. CHOICE OF LAW

12. Defendant is headquartered in Columbia, Missouri. That is the nerve center of Defendant's business activities—the place where high-level officers direct, control, and coordinate Defendant's activities, including data security, and where: (a) major policy; (b) advertising; (c) distribution; (d) accounts receivable departments; and (e) financial and legal decisions originate.

13. Data security assessments and other IT duties related to computer systems and data security occur at Defendant's Missouri headquarters. Furthermore, Defendant's response, and corporate decisions surrounding such response, to the Data Breach were made from and in Missouri. Finally, Defendant's breach of its duty to Plaintiff and Class members emanated from Missouri.

14. It is appropriate to apply Missouri law to the claims against Defendant in this case due to Defendant's significant contacts with Missouri. Defendant is headquartered in Missouri; the relevant decisions, actions, and omissions were made in Missouri; and Defendant cannot claim to be surprised by application of Missouri law to regulate its conduct emanating from Missouri.

15. To the extent Missouri law conflicts with the law of any other state that could apply to Plaintiff's claims against Defendant, application of Missouri law would lead to the most predictable result, promote the maintenance of interstate order, simplify the judicial task, and advance the forum's governmental interest.

III. PARTIES

Plaintiff Toni Reynolds

16. Plaintiff Toni Reynolds is a resident and citizen of Sacramento, California.

17. Plaintiff Reynolds received a letter dated August 4, 2022 from Defendant concerning the Data Breach.² The letter states that "unauthorized third parties gained access to certain agent user accounts and leveraged this access to run unauthorized searches in these subscription databases."³ The letter also informed Ms. Reynolds that "Cornerstone and its external agents access various subscription services, including computerized databases where driver's license information is available for the purpose of performing insurance application due

² *Cornerstone National Insurance Company Data Breach Notice to Consumers*, Office of Vermont Attorney General (Aug. 4, 2022), <https://ago.vermont.gov/blog/2022/08/05/cornerstone-national-insurance-company-data-breach-notice-to-consumers/> (last visited on Sept. 12, 2022).

³ *Id.*

diligence.”⁴ The compromised files, which Defendant obtained from motor vehicle records, contained personal information, including Plaintiff’s first and last name, driver’s license number, and any other sensitive PII Defendant had in its possession.

Defendant Cornerstone

18. Defendant Cornerstone National Insurance Company is a Missouri corporation with its principal place of business in Columbia, Missouri.⁵ Defendant Cornerstone National Insurance Company markets, sells, and underwrites automobile, homeowners, and package insurance in Oklahoma, Illinois, Tennessee, Arkansas, Kansas, and Missouri, and its websites are accessible throughout the nation.⁶

IV. FACTUAL ALLEGATIONS

A. DEFENDANT CORNERSTONE’S BUSINESS

19. Cornerstone was founded in 1997. Cornerstone describes itself as an “Insurance Support System.”⁷

20. Cornerstone has partnered with independent agents throughout the United States where they claim, “by arming your home and auto policy with the tools it needs to keep what matters safe at every turn.”⁸

21. To provide insurance to consumers, Cornerstone collects a significant amount of private information, including personal information contained in motor vehicle records that they

⁴ *Id.*

⁵ Office of the Missouri Secretary of State, Search for a Business Entity, <https://bsd.sos.mo.gov/BusinessEntity/BusinessEntityDetail.aspx?page=beSearch&ID=556790>, (last visited Sept. 12, 2022).

⁶ Cornerstone National Insurance Company, <https://www.cornerstonenational.com/>, (last visited Sept. 12, 2022).

⁷ Cornerstone National Insurance Company, *About*, <https://www.cornerstonenational.com/about>, (last visited Sept. 12, 2022).

⁸ *Id.*

obtain from governmental agencies and consumers. According to Defendant's "Privacy Notice," this information goes even beyond the scope of the information compromised in the Data Breach.⁹

22. This information includes:

- a. Name;
- b. Phone number;
- c. E-Mail address;
- d. Driver's license number;
- e. Social Security number;
- f. Date of birth;
- g. Marital status;
- h. Vehicle information;
- i. "information about other drivers";
- j. Consumer report information ("information ... obtain[ed] from third party consumer reporting agencies");
- k. Transaction information (insurance policy information, claims history, billing and payment information);
- l. "information from your transactions with us, our affiliates, or nonaffiliated third parties," and;
- m. Website information (information obtained in part from cookies, such as "Internet Protocol (IP) address, operating system, and session ID").

23. All of this information is extremely valuable.

24. In the course of collecting PII from consumers, including personal information Defendant obtains from their motor vehicle records directly from the relevant departments of motor vehicles, including Plaintiff's personal information, Defendant promised to provide

⁹Cornerstone National Insurance Company, *CNI Privacy Policy*, (June, 2021), [https://f.hubspotusercontent10.net/hubfs/6858667/CNI%20Documents/CNI%20Privacy%20Policy%20\(6-21\)%20-%20Website%20and%20Portal.pdf](https://f.hubspotusercontent10.net/hubfs/6858667/CNI%20Documents/CNI%20Privacy%20Policy%20(6-21)%20-%20Website%20and%20Portal.pdf) (last visited Sept. 12, 2022).

confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures.

25. By obtaining, collecting, using and deriving benefits from Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting this PII from unauthorized disclosure.

26. Plaintiff and the Class members reasonably relied (directly or indirectly) on this sophisticated company, with hundreds of thousands, if not millions, of individuals nationwide to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Consumers, in general, demand security to safeguard their PII, especially when driver's license numbers and other sensitive PII is involved.

27. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class members' PII from involuntary disclosure to third parties.

B. THE DATA BREACH

28. In August of 2022, Defendant first began notifying Class members about a widespread data breach of its computer systems involving the sensitive PII of consumers. According to Defendant's Notice of Data Event (hereinafter, the "Notice"), it claims it first learned of the Data Breach on November 29, 2021 when it "became aware that an authorized third party gained access to certain agent user accounts and leveraged this access to run unauthorized searches in these subscription databases."¹⁰ According to the Notice, Defendant concluded its investigation on July 6, 2022, but waited until August 4, 2022 to begin notifying impacted persons.

29. Plaintiff received the Notice on or about August 4, 2022. The Letter stated that her PII may have been compromised and included the following information listed below:

¹⁰ *Cornerstone National Insurance Company Data Breach Notice to Consumers*, Office of Vermont Attorney General (Aug. 4, 2022), <https://ago.vermont.gov/blog/2022/08/05/cornerstone-national-insurance-company-data-breach-notice-to-consumers/> (last visited on Sept. 12, 2022).

What Happened and What Information was involved?

Cornerstone National Insurance Company (“Cornerstone”) is an insurance company located in Missouri. Through its policy management software, Cornerstone and its external agents access various subscription services, including computerized databases where driver’s license information is available for the purpose of performing insurance application due diligence.

On November 29, 2021, Cornerstone became aware that an unauthorized third party gained access to certain agent user accounts and leveraged this access to run unauthorized searches in these subscription databases. Cornerstone immediately issued a global password reset and notified its software vendor, who conducted a forensic investigation to confirm security. Once the environment was secure, we moved forward with a comprehensive analysis into the extent of unauthorized activity.

These investigations, which concluded on July 6, 2022, determined that the following personal information could have been accessed by an unauthorized third party: first name, last name, and driver’s license number.

We have not received information of a specific misuse of personal information.

* * *

What you can do.

To enroll in monitoring services at no charge, please log on to <https://response.idx.us/cornerstone> and follow the instructions provided. When prompted please provide the following enrollment code to receive services: . . . IDX is available Monday through Friday, 9:00 am – 9:00 pm EST. Please note the deadline to enroll is **November 4, 2022**.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

30. From the Notice it is clear that Defendant either does not know when the Data Breach occurred or it is not being forthright about when it occurred, as Defendant only informed the Class of the date on which it became aware that an unauthorized third party gained access to its systems and their PII, not when that access actually occurred.

31. Despite discovering that an unauthorized third party gained access to its systems and Plaintiff's and Class members' PII in November 2021, Defendant spent nearly seven and a half months "investigating" the Data Breach and then waited a full additional month to notify Plaintiff and Class members of that Data Breach. During these eight and a half months, Plaintiff's and Class members' PII was exposed and accessed by cybercriminals and the Class members were left entirely unaware they faced the substantial risks and harms caused by such exposure.

32. The PII contained in the files accessed by cybercriminals in the Data Breach was not encrypted.

33. As a result of the Data Breach and Cornerstone's lackadaisical attitude towards notifying Plaintiff and Class members about it, 232,391 people had their PII exposed and potentially used for identity theft and fraud by cybercriminals for eight and a half months without their even knowing about it.

34. Plaintiff and Class members have suffered ascertainable harm and losses including, but not limited to, out-of-pocket expenses and the value of their time incurred to mitigate the effects of the attack and the present and imminent harm caused by the compromise of their sensitive personal information.

35. Plaintiff and Class members had a reasonable expectation that Defendant would comply with its obligations to implement and use adequate data security measures to keep their personal information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the Data Breach.

C. THE DATA BREACH WAS FORESEEABLE

36. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the insurance industry preceding the date of the breach.

37. Data breaches, especially those perpetrated against the insurance sector of the economy, have become increasingly widespread.

38. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.¹¹

39. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.¹² Thus, Defendant's operation in the financial sector significantly, and predictably, increased its risk of being targeted by cyber criminals.

40. Cybercriminals were also becoming more effective. In 2019, financial sector data breaches exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.¹³

41. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years, including high-profile breaches for Equifax, Target, and various healthcare systems.¹⁴

42. In 2021 alone, drivers' license numbers were taken from auto-insurance providers by cybercriminals in attacks on many companies in Defendant's industry, including GEICO, Farmers, USAA, Kemper, Metromile, and American Family. This targeting of the auto-insurance industry demonstrates that the PII companies like Defendant possess is in high demand by cybercriminals and also that sophisticated insurance companies like Defendant knew or should have known that its security practices were of particular importance to safeguard consumer data.

¹¹2019 End of Year Data Breach Report, Identity Theft Center (2019), https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Sept. 12, 2022)

¹² *Id.*

¹³ *Id.* at 15.

¹⁴ Michel Hill and Dan Swinhoe, *The 15 biggest data breaches of the 21st century*, CSO, (Sept. 12, 2021), available at <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html> (last visited Sept. 12, 2022).

43. In the first half of 2021, there were 846 data breaches in the country, on pace to set a new record. These data breach incidents impacted nearly 52.8 million individuals.¹⁵

44. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

45. Therefore, the universal increase in such attacks, and attendant high risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

46. The New York Department of Financial Services (“NYDFS”), in its February 16, 2021 industry letter recommended the following steps for entities that maintain public-facing websites:

- a. Conduct a thorough review of public-facing website security controls, including but not limited to a review of its Secure Sockets Layer (SSL), Transport Layer Security (TLS), and HTTP Strict Transport Security (HSTS and Hypertext Markup Language (HTML) configurations.
- b. Review public-facing websites for browser web developer tool functionality. Verify and, if possible, limit the access that users may have to adjust, deface, or manipulate website content using web developer tools on the public-facing websites.
- c. Review and confirm that its redaction and data obfuscation solution for NPI is implemented properly throughout the entire transmission of the NPI until it reaches the public-facing website.

¹⁵*Data Breaches Are Up 38 Percent in Q2 2021; The Identity Theft Resource Center Predicts a New All-Time High by Year’s End*, Identity Theft Resource Center (July 8, 2021), <https://www.idtheftcenter.org/post/data-breaches-are-up-38-percent-in-q2-2021-the-identity-theft-resource-center-predicts-a-new-all-time-high-by-years-end/> (last visited Sept. 12, 2022).

- d. Ensure that privacy protections are up to date and effectively protect NPI by reviewing who is authorized to see NPI, which applications use NPI, and where NPI resides.
- e. Search and scrub public code repositories for proprietary code.
- f. Block the IP addresses of the suspected unauthorized users and consider a quote limit per user session.¹⁶

47. Due to the “ongoing cybercrime campaign that is a serious threat to consumers,” NYSDFS issued a Cyber Fraud Alert Follow-up on March 30, 2021. It urged “**personal lines insurers and other financial services companies to avoid displaying prefilled NPI on public-facing websites considering the serious risk of theft and consumer harm.** (Emphasis in original) We note that many of the auto insurers targeted by this cybercrime campaign have recently disabled all NPI prefill on their public-facing websites.”¹⁷

48. NYSDFS also recommended the following basic security steps be implemented:
- a. **Disable prefill of redacted NPI.** Avoid displaying prefilled NPI, especially on public facing websites.
 - b. **Install Web Application Firewall (WAF).** WAFs help protect websites from malicious attacks and exploitation of vulnerabilities by inspecting incoming traffic for suspicious activity.
 - c. **Implement CAPTCHA.** Cybercriminals use automated programs or “bots” to steal data. Completely Automated Public Turing Tests (“CAPTCHA”) attempt to detect and block bots.

¹⁶ Industry Letter, *supra*, note 1. Note that this Industry Letter was reported online on numerous websites, including: <https://digitalguardian.com/blog/public-facing-financial-services-sites-ripe-data-theft> (Feb. 23, 2021); <https://www.gravoc.com/2021/04/09/cyber-fraud-alert-issued-for-websites-collecting-npi/> (Apr. 9, 2021); and https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert (Feb. 16, 2021) (last visited on Sept. 12, 2022).

¹⁷ Industry Letter, New York Department of Financial Services Industry Letter (Mar. 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup, (last visited Sept. 12 2022).

- d. **Improve Access Controls for Agent Portals.** Agent portals typically allow agents access to consumer NPI, and robust access controls are required by DFS's cybersecurity regulation.
- e. **Training and awareness.** Employees and agents should be trained to identify social engineering attacks. Employees and agents should know not to disclose NPI, including DLNs, over the phone. Robotic scripts with grammatical errors or repeated statements used during dialogue are key identifiers of fraudulent calls.
- f. **Limit access to NPI.** Employees and agents should only have access to sensitive information that is necessary to do their job.
- g. **Wait until payments have cleared before issuing a policy.** Auto insurers should consider waiting until an eCheck, credit card, or debit card payment has been cleared by the issuing bank before generating an online policy and granting the policyholder access to NPI.
- h. **Protect NPI received from data vendors.** Ensure that APIs used to pull data files, including JSON and XML, from data vendors are not directly accessible for the internet or agent portals.¹⁸

49. "Insurance companies are desirable targets for cyber attackers because they work with sensitive data."¹⁹ In fact, according to the Verizon 2020 Data Breach Investigations Report, there were 448 confirmed data breaches in the financial and insurance industries.²⁰ That increased to 690 confirmed data breaches in the 2022 report.²¹

¹⁸ *Id.*

¹⁹Data Protection Compliance for the Insurance Industry, Ekran System (Oct. 7, 2020), <https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry> (last visited Sept. 16, 2022).

²⁰2020 Data Breach Investigations Report, Verizon, <https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf> (last visited Sept. 12, 2022).

²¹2022 Data Breach Investigations Report, Verizon, <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf> (last visited Sept. 12, 2022).

50. For these reasons, Defendant knew or should have known about these dangers and strengthened its data protection and computer system/network accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

51. Defendant knowingly refrained from implementing basic security measures to protect Plaintiff's and Class members' PI, including motor vehicle records, in spite of having control over the configuration and design of its online quoting platform.

D. DEFENDANT FAILED TO FOLLOW FTC GUIDELINES

52. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses to highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

53. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.²² The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²³

54. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

²²Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept.12, 2022).

²³ *Id.*

on the network; and verify that third-party service providers have implemented reasonable security measures.

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45.

56. Defendant failed to properly implement basic data security practices.

57. Defendant failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers’ Personally Identifiable Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Defendant was at all times fully aware of its obligation to protect the Personally Identifiable Information of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. DEFENDANT FAILED TO COMPLY WITH INDUSTRY STANDARDS

59. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

60. Other best cybersecurity practices that are standard in the Defendant’s industry, and that upon information and belief Defendant did not employ, include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

61. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

62. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

V. DEFENDANT'S BREACH

63. Defendant breached its obligations to Plaintiff and Class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches;
- b. Failing to adequately protect consumers' PII;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;
- e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,
- f. Failing to adhere to industry standards for cybersecurity.

64. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class members' PII by allowing cyberthieves to access its IT systems which contained unsecured and unencrypted PII.

65. Accordingly, as outlined below, Plaintiff and Class members now face a present and increased risk of fraud and identity theft.

VI. HARM TO CONSUMERS

66. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

67. Specifically, driver’s license numbers are incredibly valuable. “Hackers harvest license numbers because they’re a very valuable piece of information. A driver’s license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.”²⁴

68. According to national credit bureau Experian:

A driver’s license is an identity thief’s paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver’s license number, it is also concerning because it’s connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver’s license on file), doctor’s office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.

Next to your Social Security number, your driver’s license number is one of the most important pieces of information to keep safe from thieves.²⁵

69. According to cyber security specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless

²⁴Lee Matthews, *Hackers Stole Customers’ License Numbers in Months-Long Breach*, Forbes (Apr. 20, 2021), <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658> (last visited Sept. 12, 2022).

²⁵Sue Poremba, *What Should I Do If My Driver’s License Number is Stolen?* (Oct. 24, 2018) <https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/> (last visited Sept. 12, 2022).

piece of information to lose if it happens in isolation.”²⁶ However, this is not the case. As cyber security experts point out:

It’s a gold mine for hackers. With a driver’s license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.²⁷

70. Victims of driver’s license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.²⁸

71. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class members are at a present and increased risk of fraud and identity theft for many years into the future. Indeed, Plaintiff’s driver’s license number was found on the dark web following the Data Breach alleged herein.

72. Thus, Plaintiff and Class members must vigilantly guard against identity theft for many years to come.

73. Identity theft resulting from the Data Breach may not come to light for years.

74. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

75. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class members, including information obtained from motor vehicle records, and of the foreseeable consequences that would occur if Defendant’s

²⁶Scott Ikedia, *Geico Data Breach Leaks Driver’s License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO Magazine (Apr. 23, 2021), <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/> (last visited Sept. 12, 2022).

²⁷ *Id.*

²⁸*How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021 <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last visited Sept. 12, 2022).

data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

76. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

VII. HARM TO PLAINTIFF

PLAINTIFF TONI REYNOLDS' EXPERIENCE

77. Plaintiff Toni Reynolds greatly values her privacy and PII. Prior to the Data Breach, Plaintiff Reynolds took reasonable steps to maintain the confidentiality of her PII.

78. Plaintiff Reynolds received a letter dated August 4, 2022 from Defendant concerning the Data Breach. The letter stated that on November 29, 2021 unauthorized actors gained access to files on Defendant's "certain agent accounts and leveraged this access to run unauthorized searches in these subscription databases."²⁹ According to the letter, the compromised files contained Plaintiff Reynolds' first name, last name, and driver's license number.³⁰

79. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Reynolds faces, Defendant offered her a 12 month subscription to IDX credit monitoring service and identity theft recovery services with a November 4, 2022 deadline to enroll. However, Plaintiff Reynolds has not signed up for the program, as she does not trust that Defendant's chosen vendor can protect her information. Moreover, traditional credit monitoring will not protect against the likely identity theft harm that will result from a compromised driver's license.

80. In response to the Data Breach, Plaintiff Reynolds purchased identity theft protection services, paying \$23.99 per month.

²⁹*Cornerstone National Insurance Company Data Breach Notice to Consumers*, Office of Vermont Attorney General (Aug. 4, 2022), <https://ago.vermont.gov/blog/2022/08/05/cornerstone-national-insurance-company-data-breach-notice-to-consumers/> (last visited Sep. 9, 2022).

³⁰ *Id.*

81. After the Data Breach, Plaintiff Reynolds began experiencing an uptick in suspicious text and telephone calls she attributes to this Data Breach.

82. Since learning of the Data Breach, Plaintiff Reynolds has spent considerable time reviewing her bank, credit, and debit card statements. Moreover, Plaintiff Reynolds spent this time at Defendant's direction. Indeed, in the notice letter Plaintiff Reynolds received, Defendant directed her to spend time mitigating her losses with IDX, which would "help [her] resolve issues if [her] identity was compromised."³¹

83. The Data Breach has caused Plaintiff Reynolds to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Defendant has not been forthright with information about the Data Breach.

84. Plaintiff Reynolds plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

85. Additionally, Plaintiff Reynolds is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

86. Plaintiff Reynolds stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

87. Plaintiff Reynolds has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

VIII. CLASS ALLEGATIONS

88. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated. Plaintiff proposes the following Class and California Subclass definitions, subject to amendment as appropriate:

³¹ *Id.*

All persons whose Personally Identifiable Information was maintained on Defendant's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class").

All persons residing in California at the time of the Data Breach whose Personally Identifiable Information was maintained on Defendant's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "California Subclass").

89. Excluded from the Class and the California Subclass (collectively referred to herein as the "Class") are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

90. **Numerosity**. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, the Class consists of over 232,391 individuals whose sensitive data was compromised in the Data Breach.

91. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class members' Personally Identifiable Information;
- b. Whether the Defendant violated federal or state law with respect to the allegations made herein;
- c. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

- d. Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;
- e. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;
- f. Whether Defendant owed a duty to Class members to safeguard their Personally Identifiable Information;
- g. Whether Defendant breached a duty to Plaintiff and Class members to safeguard their Personally Identifiable Information;
- h. Whether computer hackers obtained Plaintiff's and Class members' Personally Identifiable Information in the Data Breach;
- i. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- j. Whether Plaintiff and Class members suffered legally cognizable injuries as a result of Defendant's misconduct;
- k. Whether Defendant's conduct was negligent;
- l. Whether Defendant violated the DPPA;
- m. Whether Defendant violated the CCPA; and
- n. Whether Plaintiff and Class members are entitled to damages, civil penalties, and/or injunctive relief;

92. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class member, was compromised in the Data Breach.

93. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel are competent and experienced in litigating class actions.

94. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class members, in that all of Plaintiff's and Class members' data was stored on the

same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

95. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

96. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

IX. COUNTS

COUNT I

VIOLATION OF THE DRIVER'S PRIVACY PROTECTION ACT

18 U.S.C. § 2721, *et seq.*

(On Behalf of Plaintiff and the Class)

97. Plaintiff realleges and incorporates by reference paragraphs 1 through 96 as if fully alleged herein.

98. The Driver's Privacy Protection Act (the "DPPA") provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a

purpose not permitted under this chapter shall be liable to the individual to whom the information pertains.” 18 U.S.C. § 2724.

99. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

100. Under the DPPA, a “‘motor vehicle record’ means any record that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.” 18 U.S.C. § 2725(1).

101. The DPPA defines “personal information” as “information that identifies an individual, including an individual’s photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information...” 18 U.S.C. § 2725(3).

102. Driver’s licenses are motor vehicle records which, and the driver’s license numbers (“driver identification number”) contained on them qualify as personal information under the DPPA.

103. Defendant obtains, uses, discloses, resells, and rediscloses personal information from its customers’ motor vehicle records that they obtain directly from motor vehicle records agencies.

104. Defendant also obtains customers’ motor vehicle records through resellers who sell such records.

105. Defendant knowingly used motor vehicle records for uses not permitted by the DPPA, including sales, and marketing, among other impermissible uses.

106. Defendant knowingly failed to protect its computer systems and/or linked their respective public websites to systems and/or networks storing, maintaining, and/or obtaining Plaintiff’s and Class members’ personal information, including the application website.

107. During the time period starting on or before November 29, 2021, Defendant made Plaintiff’s and Class members’ personal information, including driver’s license numbers, available

to thieves who removed that personal information from Defendant's computer systems. Defendant knowingly used and disclosed and/or redisclosed Plaintiff's and Class members' motor vehicle records and the personal information contained therein to thieves, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

108. As a result of the Unauthorized Data Disclosure, Plaintiff and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

COUNT II
NEGLIGENCE
(On behalf of Plaintiff and the Class)

109. Plaintiff realleges and incorporates by reference paragraphs 1-96 as if fully alleged herein.

110. Defendant obtained Plaintiff's and Class members' Personally Identifiable Information, including but not limited to their driver's license numbers, first names, and last names.

111. By collecting and storing this data, and sharing it and using it for commercial gain, Defendant had and/or voluntarily undertook a duty of care to use reasonable means to secure and safeguard this information, to prevent disclosure of the information, and to guard the information from theft.

112. Defendant's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

113. Defendant also owed a duty of care to Plaintiff and members of the Class to provide security consistent with industry standards, and to ensure that its systems and networks and the personnel responsible for them adequately protected their customers' information.

114. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Class from a data breach. Defendant

breached its duty by failing to use reasonable measures to protect Plaintiff's and Class members' Personally Identifiable Information.

115. The specific negligent acts and omissions committed by Defendant may include, but is not limited to, the following:

- a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class members' Personally Identifiable Information (including but not limited to encrypting consumers' data);
- b. failing to adequately monitor the security of its networks and systems;
- c. allowing unauthorized access to Plaintiff's and Class members' Personally Identifiable Information; and
- d. failing to recognize in a timely manner that Plaintiff's and other Class members' Personally Identifiable Information had been compromised.

116. It was foreseeable that Defendant's failure to use reasonable measures to protect and monitor the security of Personally Identifiable Information would result in injury to Plaintiff and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

117. It was therefore foreseeable that the failure to adequately safeguard Personally Identifiable Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

118. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that Defendant's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

COUNT III

NEGLIGENCE *PER SE* (On behalf of Plaintiff and the Class)

119. Plaintiff realleges and incorporates by reference paragraphs 1-96 as if fully alleged herein.

120. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

121. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

122. Defendant's duty to use reasonable security measures also arose under the DPPA, under which Defendant was required to protect the privacy, confidentiality, and integrity of driver's license information and only to use driver's license information in a permissible fashion.

123. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) along with the DPPA constitutes negligence *per se*.

124. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the DPPA, were intended to protect.

125. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) and the DPPA were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm

suffered by Plaintiff and Class members. The DPPA was similarly enacted as a direct result of failures to protect consumer privacy like those outlined above.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT IV

VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT

Cal. Civ. Code § 1798.100, *et seq.*

(On behalf of Plaintiff and the California Subclass)

127. Plaintiff realleges and incorporates by reference paragraphs 1-96 as if fully alleged herein.

128. Defendant violated section 1798.150(a) of the California Consumer Privacy Act (the "CCPA") by failing to prevent Plaintiff's and the California Subclass' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

129. The PII of Plaintiff and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant's violation of its duty under the CCPA.

130. Plaintiff and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendant's acts described above.

131. Defendant knew, or should have known, that its network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so in the event of a data breach the PII cannot be read by an unauthorized third

party. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiff and members of the California Subclass was exposed.

132. Defendant is organized for the profit or financial benefit of its owners and collects PII as defined in Cal. Civ. Code section 1798.140.

133. Plaintiff and the Class seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguard PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiff and the California Subclass. Plaintiff and the California subclass have an interest in ensuring that their PII is reasonably protected.

134. On September 16, 2022, Plaintiff's counsel mailed a CCPA notice letter to Defendant via certified mail. Plaintiff's CCPA Notice letter detailed the violations of the CCPA listed above, including Defendant's failures to adequately safeguard Plaintiff's and Class members' PII by implementing reasonable security procedures and practices. If Defendant does not "actually cure" the effects of the Data Breach, which would require retrieving the PII or securing the PII from continuing and future use, within 30 days of delivery of the CCPA notice letter (and Plaintiff believes any such cure is not possible under these facts and circumstances), Plaintiff intends to amend this complaint to seek actual damages, and statutory damages of no less than \$100 and up to \$750 per customer record subject to the Data Breach, on behalf of the California Subclass as authorized by the CCPA.

COUNT V

VIOLATIONS OF CALIFORNIA'S UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200, *et seq.*

(On behalf of Plaintiff and the California Subclass)

135. Plaintiff realleges and incorporates by reference paragraphs 1-96 as if fully alleged herein.

136. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq.*

137. Defendant stored the PII of Plaintiff and California Subclass members in its computer systems.

138. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and California Subclass members' PII secure and prevented the loss or misuse of that PII.

139. Defendant did not disclose at any time that Plaintiff's and California Subclass members' PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which Defendant had a duty to disclose.

Unlawful Business Practices

140. Defendant engaged in unlawful business acts and practices by failing to establish adequate security practices and procedures as set forth above, by soliciting and gathering the PII of Plaintiff and the California Subclass knowing that the information would not be adequately protected, and by storing the PII of Plaintiff and the California Subclass in an unsecure electronic network, all in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to undertake reasonable measures to safeguard the PII of Plaintiff and the California Subclass, as well as the FTC Act.

141. Plaintiff and California Subclass members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiff's and California Subclass members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

Unfair Business Practices

142. Defendant engaged in unfair business practices under the “balancing test.” The harm caused by Defendant’s actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant’s failure to follow basic data security protocols and failure to disclose inadequacies of Defendant’s data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and California Subclass members, directly causing the harms alleged below.

143. Defendant engaged in unfair business practices under the “tethering test.” Defendant’s actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.”). Defendant’s acts and omissions thus amount to a violation of the law.

144. Plaintiff and California Subclass members suffered injury in fact and lost money or property as the result of Defendant’s unfair business practices. Plaintiff’s and California Subclass members’ PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

145. As a result of Defendant’s unlawful and unfair business practices in violation of the UCL, Plaintiff and California Subclass members are entitled to damages, injunctive relief, and reasonable attorneys’ fees and costs.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;
- D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class members;

- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members;
- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding

- subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
 - xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- E. Ordering Defendant to pay for a lifetime of credit monitoring services for Plaintiff and the Class;
 - F. For an award of actual damages and compensatory damages, as allowable by law;
 - G. For an award of punitive damages, as allowable by law;
 - H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
 - I. Pre- and post-judgment interest on any amounts awarded; and
 - J. Such other and further relief as this court may deem just and proper.

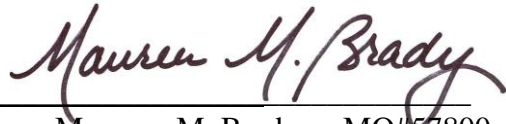
XI. JURY TRIAL DEMAND

Jury trial is demanded by Plaintiff and members of the putative Class.

DATED: September 16, 2022

Respectfully submitted,

By: Respectfully submitted,



Maureen M. Brady MO#57800
McSHANE & BRADY, LLC
1656 Washington, Ste. 120
Kansas City, MO 64108
Phone: (816) 888-8010
Fax: (816) 332-6295
E-mail:
mbrady@mcshanebradylaw.com

ATTORNEY FOR PLAINTIFF

RACHELE R. BYRD
(*pro hac vice* forthcoming)
ALEX TRAMONTANO
(*pro hac vice* forthcoming)
**WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP**
750 B Street, Suite 1820
San Diego, CA 9211
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com
tramontano@whafh.com

M. ANDERSON BERRY
(*pro hac vice* forthcoming)
GREGORY HAROUTUNIAN
(*pro hac vice* forthcoming)
**CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.**
865 Howe Avenue
Sacramento, CA 95825

Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiff